

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**

PCT

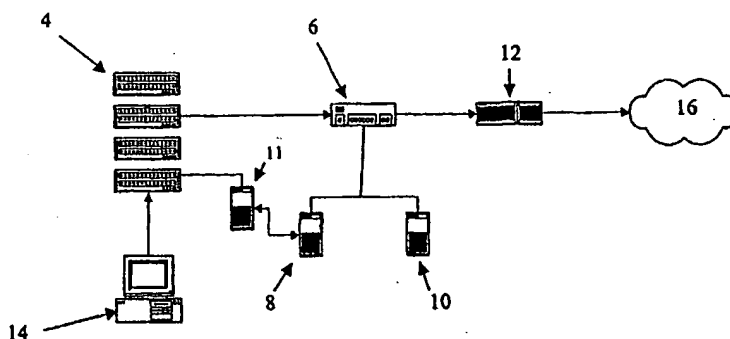
WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>7</sup> : G06F 19/00, 17/30, 12/14		A1	(11) International Publication Number: WO 00/68862 (43) International Publication Date: 16 November 2000 (16.11.00)
(21) International Application Number: PCT/AU00/00418 (22) International Filing Date: 5 May 2000 (05.05.00) (30) Priority Data: PQ 0213 6 May 1999 (06.05.99) AU PQ 3682 27 October 1999 (27.10.99) AU (71) Applicant (for all designated States except US): SHARINGA NETWORKS INC. [US/US]; 1310 King Street, Wilmington, DE 19801 (US). (72) Inventors; and (75) Inventors/Applicants (for US only): LOW, Sydney, Gordon [AU/AU]; 9 Evans Road, Kew, VIC 3101 (AU). YAN-DELL, Peter [AU/AU]; 39 Best Street, Belgrave, VIC 3160 (AU). (74) Agents: WEBBER, David, Brian et al.; Davies Collison Cave, 1 Little Collins Street, Melbourne, VIC 3000 (AU).		(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).  Published With international search report.	

(54) Title: A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM



(57) Abstract

An access system including a connection system for connecting a computer device and establishing a connection session for accessing a public communications network, such as the Internet, a switch system having a plurality of access states, one of the access states being assigned to the session for at least part of the session, each access state determining network traffic receivable by the computer device, and a session manager for managing the session and assigning at least one of the access states during the session based on connection data for the session and access requests from the computer device. The access requests include requests for TCP/IP data, such as web pages, streaming audio and video, interactive chat sessions, e-mail or FTP sites, and the access state determines whether the computer device can receive the requested TCP/IP data. The data available on the public communications network is partitioned based on the access states, and the session manager is adapted to allocate the access states to different sessions handled by the switch system simultaneously and dynamically during each session.

*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakhstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

- 1 -

## A COMMUNICATIONS NETWORK ACCESS METHOD AND SYSTEM

The present invention relates to a method and system for accessing a communications network, such as the Internet.

5

Most Internet users currently connect to the Internet via the equipment of an Internet service provider (ISP). The ISP provides remote access servers (RASs) which are able to communicate with remote computers of the users using modems and standard telephone lines. The remote computers and the RASs use standard software that executes a protocol, such as the point to point protocol (PPP), to allow the users to dial into the RASs and connect to the Internet. To achieve this, the connection or PPP software on the user's computer requires the user to enter unique authentication data, such as the user's login name and password, and this is transmitted to the ISP when the software dials and connects to the ISP equipment. If the ISP equipment determines that the authentication data is valid, the user's computer is connected and the user is allowed uninhibited access to the Internet. The user is accordingly free to view any desired web pages using a web browser on the user's computer.

10

15

The success of web sites on the Internet, particularly from a commercial perspective, is almost solely dependent on a site's ability to attract traffic to it. For this reason, a number of well known sites, such as Netscape's home page and the home pages of ISPs have been reconfigured to operate as communication "portals" to the Internet in the hope that users will continually revert to the sites to determine where to direct their browsers next. A number of sites have proved to be extremely lucrative, in the same manner as television stations which are able to attract large numbers of viewers. The current market value of companies such as Yahoo and Excite, which maintain high traffic volume sites, indicates how lucrative. As ISPs constitute a first point of connection for most Internet users, any steps or method which an ISP can implement to direct users to particular pages, rather than the user's own default home page, would be highly desirable. The present invention seeks to provide such method or at least provide a useful alternative.

20

25

30

In accordance with the present invention there is provided an access system including:

- 2 -

connection means for connecting a computer device and establishing a connection session for accessing a public communications network;

switch means having a plurality of access states, one of the access states being assigned to the session for at least part of the session, each access state determining network traffic  
5 receivable by the computer device; and

session managing means for managing the session and assigning at least one of the access states during the session based on connection data for the session and access requests from the computer device.

10 The present invention also provides an access system for a public communications network, such as the Internet, including:

means for connecting a computer device and establishing a TCP/IP session for access to the network;

switch means having a plurality of access states, the access states determining the sites  
15 and pages which can be accessed by the computer device during the session; and

means for managing the session to allocate at least one of the access states during the session.

The present invention also provides a communications network access system,  
20 including:

connection means for receiving a request from a computer device to connect to the network and for connecting the computer device to the network in response to the request;

sending means for sending login data to the computer device after it is connected to the network, the login data being adapted to generate a login display on the computer device  
25 which allows entry of unique authentication data by a user of the device; and

login means for receiving the unique authentication data entered by the user and for allowing the user to access the network using the computer device on determining that the authentication data is valid.

30 The present invention also provides a communications network access method, including:

- 3 -

establishing a TCP/IP session with a computer device; and  
assigning access states during the session, the access states determining TCP/IP data  
received by the computer device.

5       The present invention also provides a communications network access method,  
including:

connecting a computer device to a communications network;  
accessing data from affiliate locations on the network without an access charge; and  
accessing data from other locations on the network with an access charge.

10

The present invention also provides a communications network access method,  
including:

receiving a request from a computer device to connect to the network;  
connecting the computer device to the network in response to the request;  
15       sending login data to the computer device after the connecting step, the login data  
being adapted to generate a login display on the computer device allowing entry of unique  
authentication data by a user of the device;  
receiving the unique authentication data entered on the computer; and  
allowing the user to access the network using the computer device when the  
20       authentication data is validated.

The present invention also provides a communications network access method,  
including:

sending a request from a computer device to connect to a communications network,  
25       and being connected to the network in response to the request;  
receiving login data after being connected;  
generating a login display on the computer device, based on the login data, the display  
allowing entry of unique authentication data;  
sending unique authentication data entered on the computer device to the network; and  
30       obtaining access to the network after the authentication data is validated.

- 4 -

A preferred embodiment of the present invention is hereinafter described, by way of example only with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram of a preferred embodiment of a communications network access system;

5      Figure 2 is a block diagram of a server system of the access system;

Figure 3 is a flow diagram of a communications network access method of the access system;

Figure 4 is a diagram of a login page of the system and method; and

Figure 5 is a diagram of a customised home page of the system and method.

10

A communications access system, as shown in Figure 1, includes a plurality of remote access servers (RASs) 4, a layer four or higher switch 6, a database server 8, a web server system 10 and a router 12. The RASs 4 are provided to allow the computers 14 of remote users to dial into the system using standard telecommunication lines and modems and connect to the input ports of the RASs 4, respectively. On connection to a port of a RAS 4, the RAS 4 and the user's computer 14 establish a unique TCP/IP session and the IP traffic for that session is switched by the switch 6. Once the user is authenticated or approved, as described below, the user's computer 14 is allowed to access requested data on the Internet 16. The web server system 10 is used to control pages presented to a user 14 connected to the RAS 4 and handle authentication using a member profile database maintained on the database server 8, as described below. A RADIUS (Remote Authentication Dial In User Service) authentication server 11 is also provided for use in authentication. As far as the user 14 is concerned, the equipment 4, 6, 8, 10, 11 and 12 of the access system is part of the Internet.

25      The equipment 4 to 12 preferably includes standard commercially available hardware and basic database, web server and Internet access software which is known to those skilled in the art and is used in the access systems of most ISPs. The equipment 4 to 12 then also includes unique program code to manage and control each session, as discussed below. The layer four or higher switch 6 is another exception. The switch 6 is normally used by ISPs to balance the traffic handled by the RASs 4. An example of a suitable layer four switch is the AceDirector AD3™ produced by Alteon WebSystems Inc. The access system differs from that

30

- 5 -

offered by ISPs, as described below, in that the layer four switch 6 is used to connect users to the web server system 10 and control access to the Internet 16 for the users 14 on the basis of a limited number of access states encoded in the switch 6. Alternatively the unique program code and the equipment 4 to 12 could be substituted, entirely or in part, by unique integrated circuits, such as ASICs, to execute the same functions.

The switch 6 controls access to the Internet 16 by assigning an access state to each TCP session, as identified by a respective IP address. The states are each defined by one or more access rules which are encoded in the switch 6. The rules define how the switch 6 is to direct IP traffic by executing pattern matching on the received traffic. For example, the states may include a login state, a portal state, a general state, an affiliate state, a registration state, and an allow state, as described below. A rule, for example, may be receive a first URL and redirect to a second URL or the rules may allow or deny access to a predetermined set or list of URLs. The state assigned to a given IP address is controlled by a control system 20, as shown in Figure 2. The web server system 10 includes the control system 20 and a web server 22, running Apache™, which maintains web pages for the access system.

When the user 14 wishes to connect to the Internet using the access system, the user 14 dials into the system using standard PPP software and is allocated a port at the RAS 4 which answers the call. On connecting to a RAS 4, the user 14 is assigned an IP address for the IP session. The IP address is allocated from an IP address pool which depends on the number which the user dialled to connect to the RAS 4. For example, the user may have a dial-in number which provides the user with free access to Internet web sites as part of a promotion, and the user 14 is assigned an IP address and port which signifies to the switch 6 that all traffic from that IP address is to be switched directly to the router 12 and out to the Internet 16. This would occur with all IP addresses within this pool being allocated to the allow state of the switch 6, described below. Other IP addresses assigned by the RASs 4 are initially allocated to a login state of the switch until the state is changed by the control system 20. Traffic with IP addresses assigned to the login state is all redirected to the control system 20 by switch 6.

- 6 -

The control system 20, as shown in Figure 2, includes a RADIUS accounting server 30, a login server 32, a session coordinator 34, individual session managers 36, an authentication client 38, a redirector server 42 and a plan manager 44. The components 30 to 44 are all software components, but can if desired be partly or entirely replaced by application specific integrated circuits (ASICs). The control system 20 is configured to handle three different authentication scenarios:

- (i) Legacy authentication using the RADIUS authentication server 11.
- (ii) Authentication using a login display, e.g. browser based authentication.
- (iii) No authentication required.

10

For the first scenario, the user 14 dials into the RASs 4 using standard PPP software and provides a username and password. Based on the dial in number used and the configuration of the PPP software, the RAS port assigned to handle the call will direct the data provided to the RADIUS authentication server 11 to authenticate the user based on the PPP username and the password. Once authenticated, the RADIUS authentication server 11 returns a connect status message to the RAS 4 and an IP address is assigned to the user. Based on the IP address, the switch 6 forwards from the RAS 4 the connect status message, the username, calling line identification (CLI) and the IP address to the control system 20. This data is processed by the RADIUS accounting server 30 which acknowledges the new connection for the IP address and accesses the database server 8 to record the connection time for the user. The RADIUS accounting server 30 acknowledges and monitors all connections and disconnections for IP addresses, and issues connection and disconnection messages to other components in the access system. The session coordinator 34 uses the connection data, together with profile data accessed from the member profile database for the user 14, to create an instance of a session manager 36 for the connection. The connection data passed to the session coordination 34 in the connect message includes the IP address, the username and the CLI. Session managers 36 are created for each connection or session, respectively, and provide instructions to the redirector server 42 to control the state at the switch 6 for the session.

30

A session manager 36 controls the traffic which the user can receive during the session by controlling the state of the switch for the user's IP address. The state control is executed

- 7 -

on the basis of the user's member profile held in the member profile database of the server 8. The profile specifies which one of a limited number of access profiles the user belongs to. The access profiles each contain data which defines the access states that the user is able to enter. The different access states are encoded in the switch 6. On authentication of a TCP/IP session  
5 the session manager 36 for the session instructs the redirection server 42 to store data in the switch 6 indicating which one of the access states apply to the session. For example, during authentication the session is in a login state and can change to a general state or affiliate state once authentication has been completed.

10 In the second authentication scenario, the access system executes browser based authentication using the access procedure shown in Figure 3. The user is able to connect to the Internet by simply dialling into the access system using standard PPP software, at step 62, and the RASs 4 will automatically connect the user 14 without requiring the entry of any username or password. The user is automatically connected, an IP address assigned and a TCP session  
15 established, when the user dials into a port of a RAS 4 using predetermined call numbers. The system informs the user's computer 14 of the connection and the PPP software will display for the user the fact that the connection has been established and any other details associated with the connection, such as the data rate. The IP address is assigned from an address pool for immediate connection.

20 Once the user is connected to the access system the switch 6 determines whether the user's machine 14 is requesting connection to another computer on the Internet 16, at step 64. The request for example, may be simply to the user's default home page when the user opens a web browser of the computer 14. The switch 6 then determines, at step 66 by checking a  
25 stored flag representing the switch state for the IP address, whether the user has been authenticated and that the state is not the login state. If the connection session is in the login state, the switch 6 connects the user 14 to a login page on the web server 22, and the control system 20 executes a login process 68. The login process 68 is similar to that for legacy authentication, in that the RAS accounting server 30 acknowledges that connection has  
30 occurred and a new session has been established for the IP address. Data for the session is passed to the session coordinator 34 to create an instance of a session manager 36 for the

- 8 -

session. Based on the IP address, however, the session manager 36 determines that the user needs to be authenticated using browser based authentication and accordingly waits for the login server 32 to receive from the web server 22 details submitted on the login page shown in Figure 4. The login page presents the user with a number of options, which includes  
5 executing a registration process to become a new registered user, entering a username and password if already registered, or accessing help pages stored on the server 22. The page also includes a number of banner advertisements which may include links to other pages or web sites. To gain general access to the Internet 16, however, the user must enter a valid username and password combination which is authenticated by the control system 20. The login page  
10 allows the user to enter a username and password combination and then send the combination for authentication by clicking on the "sign in" button. Alternatively the combination may already be stored on the computer 14 by the user. The username and password combination is received by the session manager 36 for the session and the combination is forwarded to the authentication client 38. The authentication client 38 passes the combination to an  
15 authentication daemon 40 running on the database server 8. The authentication daemon checks the combination against stored combinations for users to determine if it is valid, identify the user and access the unique member profile for the user from the database server 8.

In the third authentication scenario, no authentication is required. In this scenario the  
20 user is allocated a telephone number to dial in on which corresponds to no authentication. The user is automatically connected, as for browser based authentication, and assigned an IP address from a pool for no authentication. Operation proceeds as described above for browser based authentication, except that the session manager 36 does not revert to the authentication client 38 to authenticate the user based on a username and password combination. The user  
25 is simply authenticated automatically by the session manager 36.

Once the user has been authenticated, either by the login process 28 or using the RADIUS server 11, an individual session manager 36 uses the member profile data for the user to compile and send a customised home page, as shown in Figure 5 to the user 14. The  
30 customised home page may also include banner advertisements, in the same manner as for the login page. The session manager 36 instructs the redirector server 42 to change the state of the

- 9 -

switch 6 to a portal state. after authentication, which directs the switch to connect to the URL for the customised home page or portal shown in Figure 5. Details concerning the user and customised home page data from the member profile are passed by the session manager 36 to the login server 32 for access by the Apache server 22 which controls compilation of the customised home page. Subsequently, the session manager 36 instructs the redirector server so as to divert the switch to one of the browsing states, either an affiliate state or a general state. For browser based authentication, as shown in Figure 3, the login authentication process is managed using the web browser of the user's machine 14, rather than the PPP software, and operation returns after the login process 68 to step 64. Accordingly, once the user reverts to step 64 and is determined at step 66 as having been authenticated, the switch 6 determines at step 70, on the basis of the access state for the session, whether the user is allowed to access a requested computer or service. If so, the user is granted access to the computer or service on the Internet 16 at step 62. If not, the user 14 is advised at step 64 of the access denial. The access denial can be communicated by connecting the user to a denial page of the Apache server 22.

A user 14 having a session which is in the affiliate state is allowed access, at no charge, to sites maintained by affiliates of the provider of the access system. The affiliate sites may be maintained on the Apache server 22 or on other servers of the Internet 16. The affiliate sites are all identified by URLs in the rules of the affiliate state. The affiliate sites can also be accessed using the links provided in the web pages of Figures 4 and 5. The rules for the affiliate state specify that access is denied to any URLs which do not belong to the affiliate sites. If however a user has a member profile that allows access to other sites on the Internet, the user is able to move to the general state. For these users, when a request is made to access a site other than an affiliate site, the user's browser is redirected by the switch 6 to an interim blank page on the Apache server 22 while the session manager 36 determines whether to instruct the redirector server 42 to change the state of the switch to the general state. The interim blank page contains code to trap the requested URL and pass the URL and a message to the login server 32 advising that the user is attempting to move from the affiliate state to the general state. This message is passed to the session manager 36, on the basis of the IP address, and the session manager 36 accesses the member's profile. If the session manager 36

- 10 -

determines on the basis of the profile that the user 14 is allowed to move the general state, a message is sent to the redirector server 42 to change the state of the switch to the general state for the session. A message is also sent from the manager 36 to the login server 32 advising that the user 14 is allowed to move to the trapped URL. The login server 32 sends a message to the  
5 Apache server 22 to forward the user 14 from the interim page to the page of the requested trapped URL. If access is denied, the URL of a denied page is used to substitute the trapped URL at the login server 32, and the user 14 is forwarded to the denial page.

Other access states are the registration state and the allow state. A session manager 36  
10 will instruct the redirector server 42 to enter the switch into the registration state for a session when a user sends a message indicating they wish to register with the access system. This may be done when, for example, the user selects the registration option on the login page of Figure 4. In the registration state the switch 6 redirects the user 14 to registration pages on the Apache server 22 and the control system 20 collects the requested details on the pages from the user  
15 14 for the user file in the database server 8. The user file normally includes the member profile data for the user which is initially established on the basis of the requested details. A session manager 36 will instruct the redirector server to cause the switch 6 to enter the allow state when the IP address indicates that the user 14 is to be provided with unrestricted access to the Internet 16 without any monitoring or charge.

20

When the session is disconnected, the RAS 4 communicates disconnection to the RADIUS accounting server 30, which in turn advises the session manager 36. The manager 36 instructs the redirector server 42 to change the state of the switch to the login state for the IP address of the disconnected session.

25

The manner in which the user is charged is controlled by a plan manager 44 that is accessed by the session manager 36. The plan manager 44 maintains different charging plans which can be applied to users. For example, all users would not be charged for access to affiliate sites, but the rate of charge may differ for accesses when in the general state. For  
30 instance, users may be allocated a predetermined period of free access for pages to the general state and then charged at a set rate thereafter. The plan manager specifies the times and rates

- 11 -

for the different plans, and this is accessed by the session managers 36 which monitor the time a user spends in different access states. The ultimate charge for a session is compiled by the session managers 36 and then stored against the user's file in the database server 8.

5           In addition to the hardware and software configuration variations for the access system discussed above, the operations executed by the switch 6 can be implemented by the following different system configurations. Firstly, the switch 6 can be replaced by a layer four switch and a proxy server. The layer four switch redirects all traffic from the RASs 4 to the proxy server which is connected to the router 12. The proxy server is also connected to the control system  
10 20. The proxy server 10 is used to establish the different access states for each connection session, with the states being dynamically adjusted under the control of the control system 20. The proxy server also stores the rules defining each of the access states which it can provide for different sessions. Another alternative, instead of encoding the access states in the switch 6, is to provide software control logic with the switch 6 to define the different access states and  
15 store the associated rules for the states, and thereby handle redirection of traffic to the web server 22 or a proxy server, as required, depending on the access state and access requests made. The control logic communicates with the control system 20, as discussed above, to dynamically adjust the access states for different sessions.

20           The access method and system are particularly advantageous as they allow ISPs, at least initially, to dynamically control the pages viewed by a user. As a minimum, the user must, and cannot avoid, viewing the login or customised home page, as these are an integral part of the login process. This allows the ISP to present advertising information, and in particular present targeted advertising information based on the user's profile, which the ISP  
25 can guarantee that all of its users will not be able to avoid. The login and customised home pages therefore act as an entry portal for all users.

By also allowing all users to connect to the system, including users who are not registered, the ISP is able to present and provide free access to selected and predetermined  
30 Internet content and services. For example, the login page may include links to certain web pages that provide banking, stock trading or home shopping, and the user will not have to pay

- 12 -

any fees to the ISP to access these pages. This allows the ISP to act as a free content provider for certain content, whilst charging a user to access other data on the Internet. To provide information to advertisers associated with the free content, the ISP can, if desired, still require and obtain certain information on and from users before providing the free content, and  
5 monitor their access.

Encoding the access states in the switch 6 also allows the ISP to restrict or allow access to selected content or services on the Internet, such as sports betting, adult orientated content or children's content.

10

Many modifications will be apparent for those skilled in the art without departing from the scope of the present invention as herein described with reference to the accompanying drawings.

- 13 -

CLAIMS:

1. An access system including:  
connection means for connecting a computer device and establishing a connection  
5 session for accessing a public communications network;  
switch means having a plurality of access states, one of the access states being assigned  
to the session for at least part of the session, each access state determining network traffic  
receivable by the computer device; and  
session managing means for managing the session and assigning at least one of the  
10 access states during the session based on connection data for the session and access requests  
from the computer device.
2. An access system as claimed in claim 1, wherein the session managing means is  
adapted to dynamically assign and adjust the access states during the session.
- 15 3. An access system as claimed in claim 1, wherein the access states are defined by rules  
which determine locations of the network accessible by the computer device.
4. An access system as claimed in claim 3, wherein the switch means is adapted to  
20 redirect the computer to a predetermined network location based on the access state for the  
session.
5. An access system as claimed in claim 1, wherein the session is a TCP/IP session and  
the connection data includes an IP address for the session and/or profile data stored in the  
25 system for a user of the computer device.
6. An access system as claimed in claim 5, wherein the access requests include requests  
for TCP/IP data, such as web pages, streaming audio and video, interactive chat sessions, e-  
mail or FTP sites, and the access state determines whether the computer device can receive the  
30 requested TCP/IP data.

- 14 -

7. An access system as claimed in claim 1, wherein data available on the public communications network is partitioned based on the access states, and the session managing means is adapted to allocate the access states to different sessions handled by the switch means simultaneously and dynamically during each session.
8. An access system as claimed in claim 7, wherein the session managing means includes a connection manager to manage connection and disconnection of each session, a session coordinator to establish a session manager for each session, and session managers for each session to process the access requests collected by the access system and assign access states for the sessions.
9. An access system as claimed in claim 1, wherein the access states include an affiliate access state that restricts access to locations on the network affiliated to a provider of the access system.
10. An access system as claimed in claim 1, wherein the access states include a portal state that connects the computer device to a predetermined portal page.
11. An access system as claimed in claim 1, wherein the access states include a login state, a registration state, a general browsing state which allows access to all locations on the network, and an allow state which allows access to all locations on the network without the user of the computer device providing authentication data.
12. An access system as claimed in claim 1, wherein the session managing means is adapted to allocate a number of the access states at respective times during the session.
13. An access system as claimed in claim 11, wherein on disconnection of the session, the switch means reverts to the login access state.

- 15 -

14. An access system for a public communications network, such as the Internet, including:  
means for connecting a computer device and establishing a TCP/IP session for access  
to the network;

switch means having a plurality of access states, the access states determining the sites  
5 and pages which can be accessed by the computer device during the session; and  
means for managing the session to allocate at least one of the access states during the  
session.

15. A communications network access system, including:

10 connection means for receiving a request from a computer device to connect to the  
network and for connecting the computer device to the network in response to the request;

sending means for sending login data to the computer device after it is connected to  
the network, the login data being adapted to generate a login display on the computer device  
which allows entry of unique authentication data by a user of the device; and

15 login means for receiving the unique authentication data entered by the user and for  
allowing the user to access the network using the computer device on determining that the  
authentication data is valid.

16. A communications network access system as claimed in claim 15, wherein the  
20 connection means includes a switch having a set of access states encoded therein and the login  
means accesses profile data for the user to control access to the network using the switch and  
the profile data to determine one of the access states for the switch.

17. A communications network access system as claimed in claim 16, wherein the  
25 connection means includes a RAS.

18. A communications network access system as claimed in claim 17, wherein the sending  
means and login means includes a web server and a user database.

30 19. A communications network access method, including:

- 16 -

establishing a TCP/IP session with a computer device; and  
assigning access states during the session, the access states determining TCP/IP data  
received by the computer device.

- 5    20.    A communications network access method, including:  
         connecting a computer device to a communications network;  
         accessing data from affiliate locations on the network without an access charge; and  
         accessing data from other locations on the network with an access charge.
- 10   21.    A communications network access method, including:  
         receiving a request from a computer device to connect to the network;  
         connecting the computer device to the network in response to the request;  
         sending login data to the computer device after the connecting step, the login data  
         being adapted to generate a login display on the computer device allowing entry of unique  
15   authentication data by a user of the device;  
         receiving the unique authentication data entered on the computer; and  
         allowing the user to access the network using the computer device when the  
         authentication data is validated.
- 20   22.    A communications network access method as claimed in claim 21, including accessing  
         profile data for the user and controlling access to the network using the profile data.
23.    A communications network access method as claimed in claim 22, wherein the profile  
         data determines one of a set of access states encoded in a switch connecting the computer  
25   device to the network.
24.    A communications network access method as claimed in claim 23, wherein the login  
         display includes links to locations on the communications network for which entry of the  
         authentication data is not required.

- 17 -

25. A communications network access method, including:  
    sending a request from a computer device to connect to a communications network,  
    and being connected to the network in response to the request;  
    receiving login data after being connected;
- 5      generating a login display on the computer device, based on the login data, the display  
allowing entry of unique authentication data;  
    sending unique authentication data entered on the computer device to the network: and  
    obtaining access to the network after the authentication data is validated.
- 10 26. Computer software including code for executing the steps of the method as claimed  
in any one of claims 19 to 25.

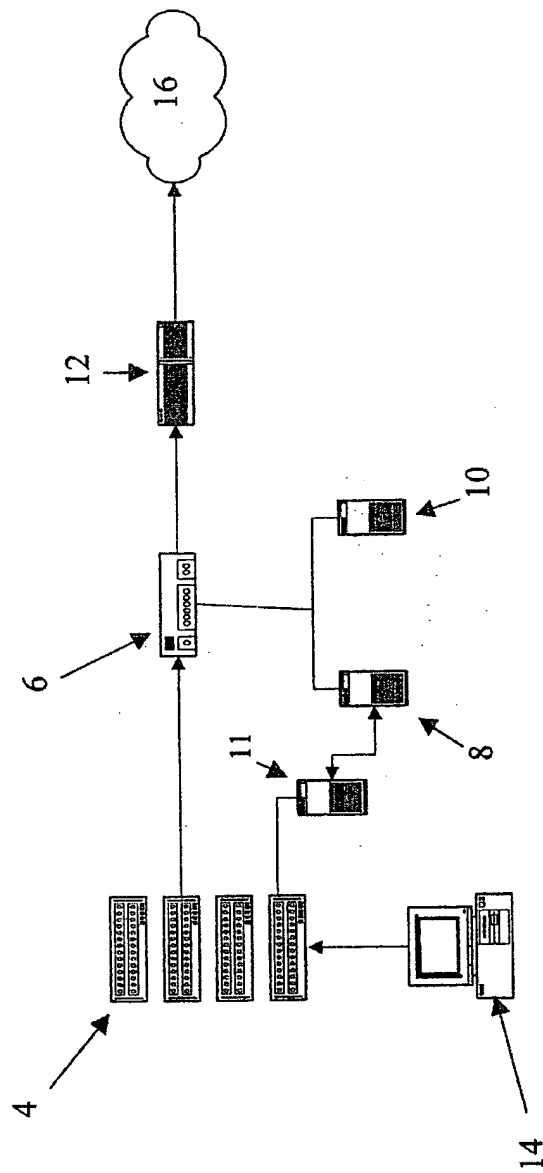


Figure 1

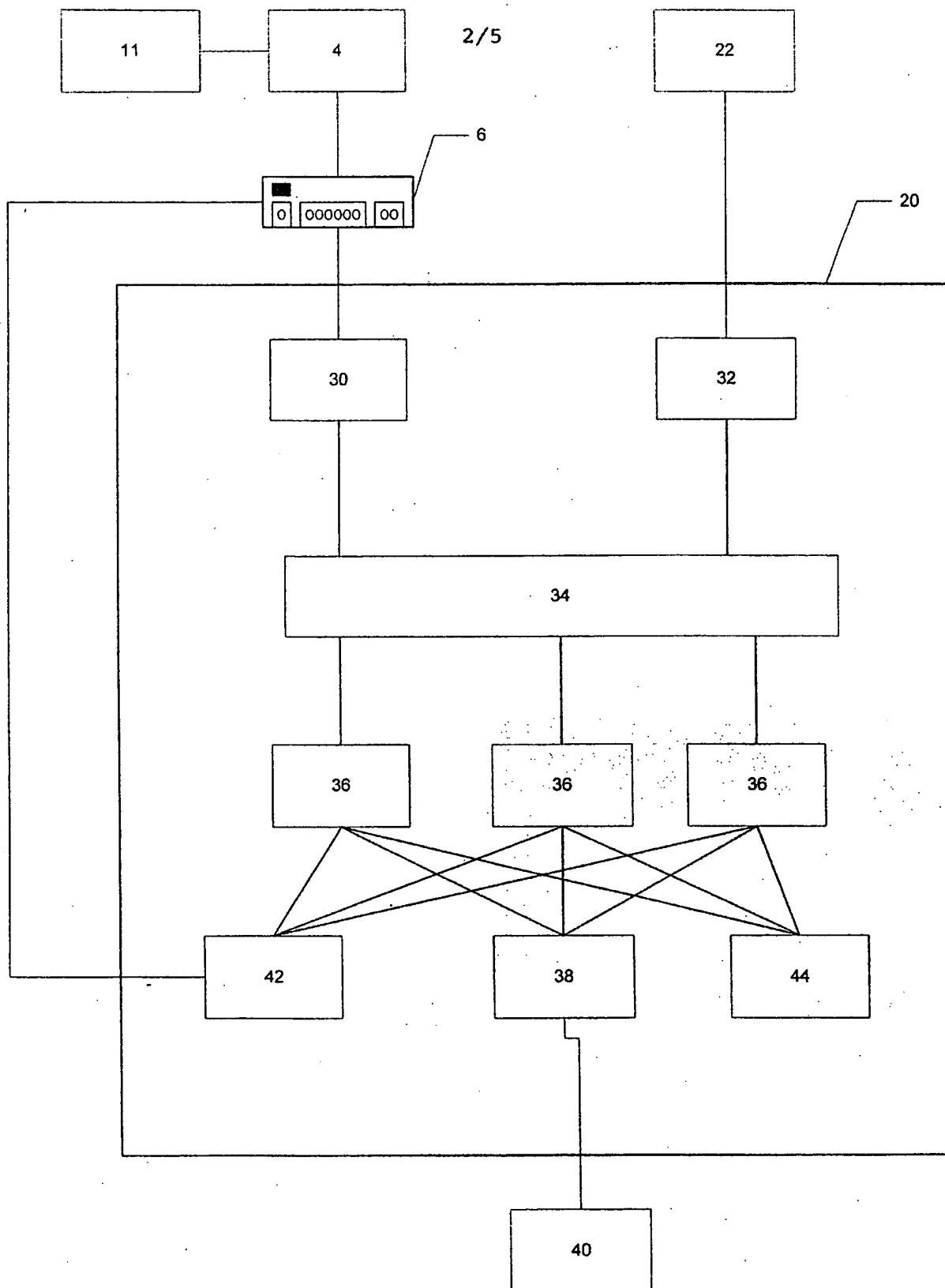
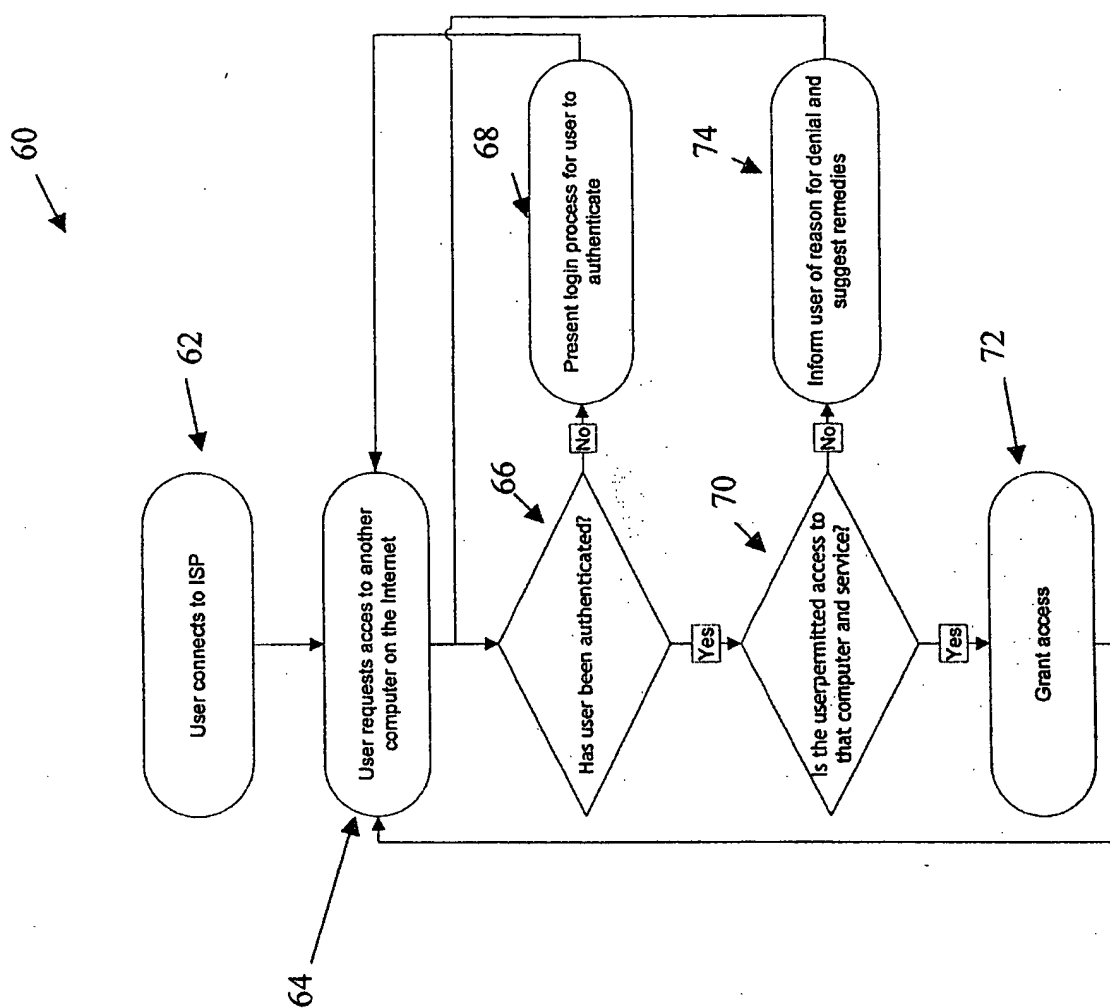


Figure 2

Figure 3



NetScape 4.08 In page

Back Forward Reload Home Search Netscape Print Security Stop

# Please Sign In

**I'm a New User**

**Sign me up!**

**I'm already registered**

Username:

Password:

☐ Save my ID & Password (What's this?)

**Need help?**

**Go to help pages**

**What's New Today**

**amazon.com**

CLICK HERE

**The smart way to buy your next car**

**Click here to apply online...**

**WELLS FARGO**

**YAHOO! OPEN 24 HOURS A DAY SHOPPING**

Online Home Loan Applications Click Here

Figure 4

Back Forward Reload Home Search Netscape Images Print Security Stop

Netscape Customised Offers Page

# Your Special Offers:

**Register for the...**

**ANSETT AUSTRALIA**

**Fly return to Hong Kong\* for only \$935**

**GetawayTravel**

**IT'S YOUR RETIREMENT. DO YOU KNOW?**

**GO RETIREMENT WITH BARNARD**

**1. TAKE 2 MINUTES**

**2. APPLY**

**click here to apply for the Platinum Yahoo! VISA CARD**

# Your Favourite Sites:

[EBIZ standard newbytes Newspace PRNews Net CMP MSNBC](#)  
[Hotwired Yahoo! - Tech Reuters ABC News BBC | News](#)  
[EvngStd W, Mel, Syd AFR](#)

Figure 5

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU00/00418

<b>A. CLASSIFICATION OF SUBJECT MATTER</b>		
Int. Cl. <sup>7</sup> : G06F 19/00, 17/30, 12/14		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b>		
Minimum documentation searched (classification system followed by classification symbols) G06F/-		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched AU:IPC AS ABOVE		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) WPAT, JAPIO		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9841913A, BASCOM GLOBAL INTERNET SERVICES, 24 September 1998.	15,21,25
X	page 11, figure 3	20
X	pages 2,6,13,14, figure 6	
X	WO 9642041A, OPEN MARKET INC., 27 December 1996	15,19,20,21, 25
	abstract, pages 4-8	
P,X	WO 9959375A, TELEFONAKTIEBOLAGET LM ERICSSON, 18 November 1999	15,21,25
	abstract, claim 1	
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C <input checked="" type="checkbox"/> See patent family annex		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 14 June 2000		Date of mailing of the international search report 20 JUN 2000
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaaustralia.gov.au Facsimile No. (02) 6285 3929		Authorized officer  S KAUL Telephone No : (02) 6283 2182

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU00/00418

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5560008A, JOHNSON et al, 24 September 1996	
A	US 5696898A, BAKER et al, 9 December 1997	
A	US 5889958A, WILLENS, 30 March 1999	

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/AU00/00418

## **Box I** Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos :  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2. ☐ Claims Nos :  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
3. ☐ Claims Nos :  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

## **Box II** Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claims 1-14,16-20 relate to selective access of the communications network.

Claims 15,21,22,25 relate to an arrangement for login to the communications network based on receipt of authentication data.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims: it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☐ No protest accompanied the payment of additional search fees.

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
**PCT/AU00/00418**

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report				Patent Family Member			
WO	9841913	AU	65648/98	US	5987606		
WO	9642041	AU	59367/96	CA	2221506	EP	830774
		US	5708780	US	5812776		
US	5560008	BR	9002267	EP	456920	JP	3009444
US	5696898	CA	2196867	CN	1159324	EP	793826
		WO	9715008				
US	5889958	AU	57121/98	WO	9828690		
END OF ANNEX							